Two-Round Concurrent 2PC from Sub-Exponential LWE

Behzad Abdolmaleki[1], Saikrishna Badrinarayanan[2⋆], Rex Fernando[3⋆], Giulio Malavolta[4,5], Ahmadreza Rahimi[5], and Amit Sahai[6]

[1] University of Sheffield, UK
behzad.abdolmaleki@sheffield.ac.uk
[2] LinkedIn, USA
bsaikrishna7393@gmail.com
[3] Carnegie Mellon University, USA
rex1fernando@gmail.com
[4] Bocconi University, Italy
[5] Max Planck Institute for Security and Privacy, Germany
{giulio.malavolta, ahmadreza.rahimi}@mpi-sp.org
[6] UCLA, USA
sahai@cs.ucla.edu

Abstract. Secure computation is a cornerstone of modern cryptography and a rich body of research is devoted to understanding its round complexity. In this work, we consider two-party computation (2PC) protocols (where both parties receive output) that remain secure in the realistic setting where many instances of the protocol are executed in parallel (concurrent security). We obtain a two-round *concurrent-secure* 2PC protocol *based on a single, standard, post-quantum* assumption: The subexponential hardness of the learning-with-errors (LWE) problem. Our protocol is in the plain model, i.e., it has no trusted setup, and it is secure in the super-polynomial simulation framework of Pass (EUROCRYPT 2003). Since two rounds are minimal for (concurrent) 2PC, this work resolves the round complexity of concurrent 2PC from standard assumptions.

As immediate applications, our work establishes feasibility results for interesting cryptographic primitives, such as the first two-round password authentication key exchange (PAKE) protocol in the plain model and the first two-round concurrent secure computation protocol for quantum circuits (2PQC).

1 Introduction

Secure computation is a fundamental primitive in cryptography which allows two or more parties, all of whom have private inputs, to collectively compute some function over their inputs securely without revealing the inputs themselves. In recent years, significant attention has been devoted to the round-complexity of

⋆ Part of the work was done while the author was affiliated with UCLA.